PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-301857
(43)Date of publication of application : 13.11.1998

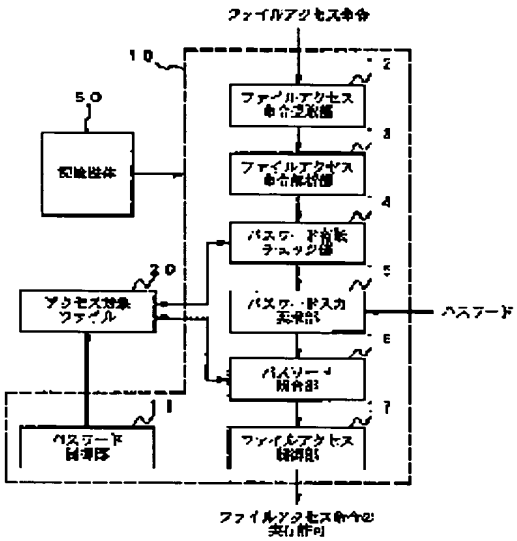
(51)Int.Cl. G06F 12/14
G06F 12/00

(21)Application number : 09-123504
(22)Date of filing : 25.04.1997

(71)Applicant : NEC CORP
(72)Inventor : MATSUI SHINICHI

(54) FILE SECURITY PROTECTING CIRCUIT

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a file security protecting device capable of protecting the security of confidential data stored in an easily attachable/detachable storage medium and permitting access to non-confidential data stored in the storage medium to a user who does not deal with the confidential data.
SOLUTION: This circuit is provided with a file access instruction analyzing part 13 which analyzes an access instruction, and specifies a data file being the object of access, password input requesting part 15 which requests the input of a password when the data file specified by the file access instruction analyzing part 13 is a data file whose password is set, password collating part 16 which judges whether or not a password inputted in response to the request of the password input requesting part 15 is legal, and file access controlling part 17 which permits the execution of an access instruction to an operating a system when it is judged that the input password is legal by the password collating part 16.



LEGAL STATUS

[Date of request for examination] 25.04.1997
[Date of sending the examiner's decision of rejection] 17.10.2000
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平10－301857

(43)公開日　平成10年(1998)11月13日

(51)Int.Cl.[6]		識別記号	FI		
Ｇ０６Ｆ	12/14	３２０	Ｇ０６Ｆ	12/14	３２０Ｃ
	12/00	５３７		12/00	５３７Ｄ

審査請求　有　請求項の数４　ＦＤ　（全 6 頁）

(21)出願番号　特願平9－123504

(22)出願日　平成９年(1997)４月25日

(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目７番１号

(72)発明者　松井　伸一
東京都港区芝五丁目７番１号　日本電気株式会社内

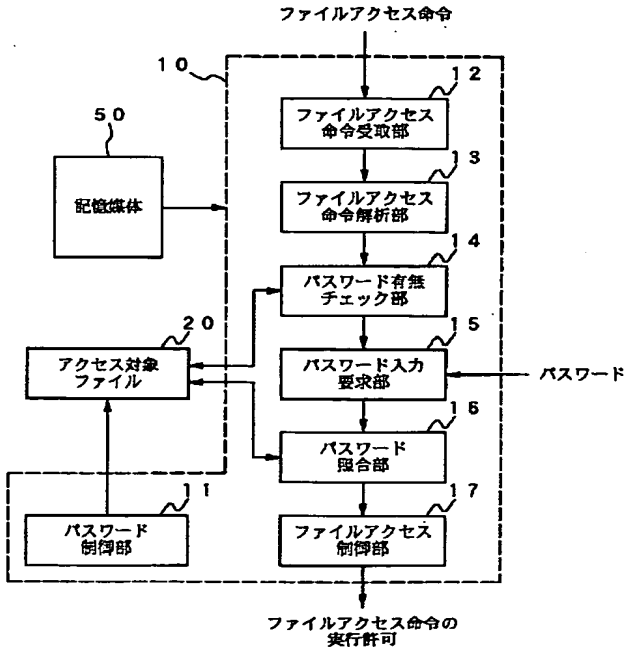
(74)代理人　弁理士　松本　正夫

(54)【発明の名称】　ファイル機密保護装置

(57)【要約】

【課題】　着脱が容易な記憶媒体に格納された機密データの機密性を保護すると共に、機密データを扱わない利用者に対して当該記憶媒体に格納された非機密データへのアクセスを許可するファイル機密保護装置を提供する。

【解決手段】　アクセス命令を解析してアクセス対象のデータファイルを特定するファイルアクセス命令解析部１３と、ファイルアクセス命令解析部１３により特定されたデータファイルが、パスワードを設定されたデータファイルである場合に、当該パスワードの入力を要求するパスワード入力要求部１５と、パスワード入力要求部１５の要求に応じて入力されたパスワードが正当かどうかを判断するパスワード照合部１６と、パスワード照合部１６により入力パスワードが正当と判断された場合に、オペレーティングシステムに対して前記アクセス命令の実行を許可するファイルアクセス制御部１７とを備える。



【特許請求の範囲】
【請求項１】　オペレーティングシステムによるデータファイルへのアクセス命令の実行を許可するかどうかを制御することにより、前記データファイルに格納された機密データの機密性を保護するファイル機密保護装置において、
外部から入力された前記アクセス命令を解析してアクセス対象のデータファイルを特定するアクセス命令解析手段と、
前記アクセス命令解析手段により特定されたデータファイルが、パスワードを設定されたデータファイルである場合に、当該パスワードの入力を要求するパスワード要求手段と、
前記パスワード要求手段の要求に応じて入力されたパスワードが正当かどうかを判断する照合手段と、
前記照合手段により入力パスワードが正当と判断された場合に、前記オペレーティングシステムに対して前記アクセス命令の実行を許可するアクセス制御手段とを備えることを特徴とするファイル機密保護装置。
【請求項２】　データファイルに対して、パスワードを設定するパスワード制御手段をさらに備えることを特徴とする請求項１に記載のファイル機密保護装置。
【請求項３】　データファイルに対して、パスワードを新規に設定すると共に、既にデータファイルに設定されているパスワードを変更し、または削除するパスワード制御手段をさらに備えることを特徴とする請求項１に記載のファイル機密保護装置。
【請求項４】　前記パスワード制御手段が、前記データファイルに格納されるデータの一部として前記パスワードを設定することを特徴とする請求項２または請求項３に記載のファイル機密保護装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、パーソナルコンピュータクラスのコンピュータのオペレーティングシステム上で実行されるファイルアクセス命令に対するデータファイルの機密保護装置に関し、特にフロッピーディスクその他の着脱の容易な記憶媒体に格納されたデータファイルの機密を保護するファイル機密保護装置に関する。
【０００２】
【従来の技術】コンピュータシステムで用いられるデータファイルにおいて、個人の情報が含まれるデータファイルのように、不特定の第三者によって自由に参照，更新，削除されることを防止する必要のある場合がある。そのため、従来から、特定のデータファイルの機密を保護すべく、ファイルアクセスの正当性をチェックする手段が提案されている。この種の従来技術として、特開平４－１７１５５４号公報に開示されたファイル機密保護装置や特開平３－９１０４７号公報に開示された情報処理システムがある。
【０００３】特開平４－１７１５５４号公報には、機密保護の対象ファイルのファイル名とパスワードとを対応させて記録したパスワード管理ファイルを備え、該パスワード管理ファイルに登録された対象ファイルに対するファイルアクセス命令を受け取った場合に、当該ファイルアクセス命令によりアクセスしようとするファイルに対するパスワードの入力を要求し、入力されたパスワードと当該ファイルに対応付けられたパスワードとを照合し、両パスワードが一致した場合にのみ当該ファイルアクセス命令をオペレーティングシステムに送ることにより、前記パスワード管理ファイルに登録されたファイルの機密を保護するファイル機密保護装置について記載されている。
【０００４】しかし、前記パスワード管理ファイルに、フロッピーディスクや光磁気ディスクその他の容易に着脱可能な記憶媒体に格納したファイルを常時的確に登録しておくことは困難である。したがって、前記パスワード管理ファイルを用いた機密保護手段では、前記着脱の容易な記憶媒体に格納したファイルに対する十分な機密保護を実現することはできなかった。
【０００５】また、特開平３－９１０４７号公報には、情報処理装置（コンピュータ）と補助記憶装置とを備え、前記情報処理装置を利用可能なユーザに関する所定の情報を格納する記憶手段を前記補助記憶装置と前記情報処理装置とに設け、前記補助記憶装置の記憶手段に記憶してある情報と前記情報処理装置の記憶手段に記憶してある情報とを照合し、双方が一致しない場合には前記補助記憶装置へのアクセスを禁止する手段を前記情報処理装置に設けた情報処理システムについて記載されている。
【０００６】しかし、この場合、前記補助記憶装置における記憶媒体単位でパスワードが設定されるため、１個の記憶媒体に機密データと非機密データとが存在する場合、機密データを扱わない利用者は、当該記憶媒体に格納されている非機密データを利用することができなかった。
【０００７】
【発明が解決しようとする課題】上述したように、従来のデータファイルの機密保護装置によれば、ファイル単位でアクセスの可否を制御する場合には、着脱が容易な記憶媒体に格納されたデータファイルに対するアクセスの可否を制御することができないという欠点があった。
【０００８】また、記憶媒体単位でアクセスの可否を制御すると、機密データを扱わない利用者が当該記憶媒体に格納されている非機密データにアクセスできないという欠点があった。
【０００９】本発明の目的は、機密データと非機密データとを格納した着脱が容易な記憶媒体を複数の利用者にて使用する場合に、記憶媒体に格納された機密データの

漏洩や改変を防止すると共に、機密データを扱わない利用者に対して当該記憶媒体に格納された非機密データへのアクセスを許可することを可能としたファイル機密保護装置を提供することである。

【００１０】

【課題を解決するための手段】上記の目的を達成する本発明のファイル機密保護装置は、オペレーティングシステムによるデータファイルへのアクセス命令の実行を許可するかどうかを制御することにより、前記データファイルに格納された機密データの機密性を保護するファイル機密保護装置において、外部から入力された前記アクセス命令を解析してアクセス対象のデータファイルを特定するアクセス命令解析手段と、前記アクセス命令解析手段により特定されたデータファイルが、パスワードを設定されたデータファイルである場合に、当該パスワードの入力を要求するパスワード要求手段と、前記パスワード要求手段の要求に応じて入力されたパスワードが正当かどうかを判断する照合手段と、前記照合手段により入力パスワードが正当と判断された場合に、前記オペレーティングシステムに対して前記アクセス命令の実行を許可するアクセス制御手段とを備えることを特徴とする。

【００１１】請求項２の本発明のファイル機密保護装置は、データファイルに対して、パスワードを設定するパスワード制御手段をさらに備えることを特徴とする。

【００１２】請求項３の本発明のファイル機密保護装置は、データファイルに対して、パスワードを新規に設定すると共に、既にデータファイルに設定されているパスワードを変更し、または削除するパスワード制御手段をさらに備えることを特徴とする。

【００１３】請求項４の本発明のファイル機密保護装置は、前記パスワード制御手段が、前記データファイルに格納されるデータの一部として前記パスワードを設定することを特徴とする。

【００１４】

【発明の実施の形態】以下、本発明の実施の形態について図面を参照して詳細に説明する。

【００１５】図１は、本発明の一実施形態によるファイル機密保護装置の構成を示すブロック図である。図２は、本実施形態のファイル機密保護装置を搭載したコンピュータシステムの構成例を示す概略図である。

【００１６】図２に示すように、本実施形態のファイル機密保護装置１０は、アプリケーションプログラム（ＡＰ）３０とオペレーティングシステム（ＯＳ）４０との間に位置する。そして、アプリケーションプログラム３０からのアクセス対象ファイル２０へのアクセス命令がオペレーティングシステム４０にわたる前に、当該アクセス命令をチェックし、機密データへのアクセスの可否を制御する。

【００１７】図１に示すように、本実施形態のファイル機密保護装置１０は、アクセス対象ファイル２０に対してパスワードの設定、変更、削除を行うパスワード制御部１１と、ファイルアクセス命令を受け取り、アクセス対象ファイル２０を参照してファイル機密保護機能を実現するファイルアクセス命令受取部１２、ファイルアクセス命令解析部１３、パスワード有無チェック部１４、パスワード入力要求部１５、パスワード照合部１６、およびファイルアクセス制御部１７とを備える。なお、図１には本実施形態における特徴的な構成のみを記載し、他の一般的な構成については記載を省略してある。

【００１８】本実施形態の各構成は、コンピュータプログラムで制御されたＣＰＵとＲＡＭその他の内部メモリとで実現される。ＣＰＵを制御するコンピュータプログラムは、図１に示す記憶媒体５０に格納されて提供される。記憶媒体５０は、磁気ディスクや半導体メモリその他の一般的な記憶媒体である。記憶媒体５０から所定の読取手段を経てコンピュータプログラムをロードすることにより、ＣＰＵにて、上述したパスワード制御部１１、ファイルアクセス命令受取部１２、ファイルアクセス命令解析部１３、パスワード有無チェック部１４、パスワード入力要求部１５、パスワード照合部１６、およびファイルアクセス制御部１７の各機能実行部が実現される。

【００１９】アクセス対象ファイル２０は、任意の補助記憶装置に格納されている。補助記憶装置の記憶媒体としては、フロッピーディスクや光磁気ディスクその他の着脱が容易な記憶媒体を含む。また、アクセス対象ファイル２０には、図２に示すように、標準的に、ファイル名２１と、ファイル名２１に対応するデータ２３とが格納されている。データ２３は、通常、複数のレコードに分割されて格納されている。ファイル名２１にはデータ２３が格納されたレコードの先頭のアドレス２２が付加され、各レコードのデータには当該データの続きが格納されたレコードを示すアドレス２４が付加されている。当該データが当該ファイル名２１に対応するデータ２３の最後である場合、続きのデータのアドレスに変えてデータ２３の終端であることを示す記号が付加される。

【００２０】アクセス対象ファイル２０に対して、アクセスできる利用者を制限するためのパスワードを設定する場合、図２に示すように、ファイル名２１に、アドレス２２の代わりに、パスワード２６を格納したレコードのアドレス２５を付加する。そして、パスワード２６に、データ２３が格納されたレコードの先頭のアドレス２２を付加する。

【００２１】パスワード制御部１１は、任意のアクセス対象ファイル２０に対して新規にパスワードを設定する場合や、設定されているパスワードを変更または削除する場合に、１つのコマンドとして起動される。パスワード制御部１１が起動したならば、利用者は、新規設定、更新、削除の動作モードの中から１つを選択する。新規

設定を選択した場合は、設定するファイル名とパスワードを入力することにより、当該アクセス対象ファイル２０に対してパスワード２６が登録される。すなわち、ファイル名２１に付加されたアドレスを、当該パスワードを格納したレコードのアドレスに変更し、パスワード２６に、データ２３が格納されたレコードの先頭のアドレス２２を付加する。これ以後、当該アクセス対象ファイル２０は、設定されたパスワードを入力しない限りアクセスすることができない。

【００２２】動作モードとして変更を選択した場合は、パスワードを変更しようとするファイル名と旧いパスワードと変更後の新しいパスワードとを入力することにより、当該アクセス対象ファイル２０のパスワード２６が更新される。これ以後、当該アクセス対象ファイル２０は、更新された新しいパスワードを入力しない限りアクセスすることができない。

【００２３】動作モードとして削除を選択した場合は、パスワードを削除しようとするファイル名とパスワードとを入力することにより、当該アクセス対象ファイル２０に設定されていたパスワード２６が削除される。すなわち、パスワード２６を格納したレコードを消去し、ファイル名２１に付加されたパスワードを格納していたレコードのアドレス２５がデータ２３を格納するレコードの先頭のアドレス２４に変更される。これ以後、当該アクセス対象ファイル２０は、パスワードなしでアクセスできることとなる。

【００２４】ファイルアクセス命令受取部１２は、アプリケーションプログラム３０から発行されたアクセス対象ファイル２０へのアクセス命令を入力し、バッファにセーブする。

【００２５】ファイルアクセス命令解析部１３は、ファイルアクセス命令受取部１２によってバッファにセーブされたファイルアクセス命令の種類（例えば、ファイル作成、読み取り、更新、削除）とアクセス対象ファイル２０のファイル名とを解析する。

【００２６】パスワード有無チェック部１４は、ファイルアクセス命令解析部１３による解析結果に基づいてアクセス対象ファイル２０を参照し、ファイル名に付加されたアドレスを検索して、当該アドレスのレコードに格納されたデータがパスワードかどうかを確認する。パスワードである場合はパスワード入力要求部１５に制御を渡し、パスワードでない場合は当該ファイルアクセス命令をオペレーティングシステム４０に転送する。

【００２７】パスワード入力要求部１５は、ファイルアクセス命令が正当なものか否かを判断するため、パスワードの入力要求を行い、入力されたパスワードを専用のバッファにセーブする。パスワードの入力要求は、例えば、ディスプレイ装置にパスワードの入力を要求するメッセージを表示したり、音声により利用者に通知したりすることにより行う。パスワードの入力は、キーボードその他の入力デバイスを用いて行う。

【００２８】パスワード照合部１６は、パスワード入力要求部１５により専用バッファにセーブされたパスワードとアクセスしようとするアクセス対象ファイル２０に登録されているパスワード２６とを照合する。

【００２９】ファイルアクセス制御部１７は、パスワード照合部１６によるパスワードの照合結果においてパスワードが一致した場合に、ファイルアクセス命令の実行を許可し、ファイルアクセス命令受取部１２で受け取ってバッファにセーブされたファイルアクセス命令をオペレーティングシステム４０に転送して実行させる。一方、パスワードが一致しなかった場合は、エラーメッセージ出力命令を発行してオペレーティングシステム４０に送り、利用者に対してエラーメッセージを通知する。エラーメッセージの通知は、ディスプレイ装置への表示や音声により行う。なお、実行を許可したファイルアクセス命令が当該アクセス対象ファイル２０を削除するものであれば、当該アクセス対象ファイル２０のパスワード２６を格納したレコードも共に削除する。

【００３０】次に、図３のフローチャートを参照して本実施例によるアクセス対象ファイルへのアクセス制御の動作について説明する。

【００３１】まず、ファイルアクセス命令受取部１２が、アプリケーションプログラム３０から発行されたファイルアクセス命令を受け取ると（ステップ３０１）、ファイルアクセス命令解析部１３が、当該ファイルアクセス命令を解析する（ステップ３０２）。

【００３２】次に、パスワード有無チェック部１４が、ファイルアクセス命令解析部１３による解析結果に基づいて、アクセスしようとするアクセス対象ファイル２０を参照し、パスワードが設定されているかどうかを確認する（ステップ３０３）。パスワードが設定されていなければ、当該アクセス対象ファイル２０はアクセス可能な利用者を制限していないので、オペレーティングシステム４０に当該ファイルアクセス命令を送り、当該アクセス対象ファイル２０へのアクセスを実行させる（ステップ３０４、３０９）。

【００３３】一方、パスワードが設定されているならば、パスワード入力要求部１５によるパスワード入力要求処理に移行する（ステップ３０４、３０５）。パスワードが入力されたならば、パスワード照合部１６がアクセス対象ファイル２０を参照し、パスワードの照合を行って、入力されたパスワードが正当かどうかを判断する（ステップ３０６、３０７）。入力されたパスワードが正当であれば、当該アクセス対象ファイル２０へのアクセスが許可されているため、オペレーティングシステム４０に当該ファイルアクセス命令を送り、当該アクセス対象ファイル２０へのアクセスを実行させる（ステップ３０８、３０９）。

【００３４】入力されたパスワードが不正である場合

は、エラーメッセージを出力して処理を終了する（ステップ３０８、３１０）。

【００３５】次に、パスワードを付加したアクセス対象ファイルを着脱可能な記憶媒体に格納した場合のアクセス制御の動作について説明する。

【００３６】上述したように、アクセスを許可するためのパスワードは、アクセス対象ファイル２０自体に登録されるため、アクセス対象ファイル２０が格納されている記憶媒体の種類は何ら問題とならない。したがって、本実施形態によるファイル機密保護装置を備えるコンピュータシステムでは、上述の通りの動作によりアクセス制御が行われる。

【００３７】これに対し、本発明のファイル機密保護装置を有しないコンピュータシステムでは、上述したようなパスワードに基づくアクセス制御を行うことはできない。しかし、パスワードを付加したファイルを参照しようとした場合、ファイル名にはデータの先頭位置のアドレスの代わりにパスワードのアドレスが付加されており、パスワードもデータの一部とみなされることにより、データの配置がずれるため、データの内容を正しく参照することができない。このため、データを改変することもできない。

【００３８】以上好ましい実施例をあげて本発明を説明したが、本発明は必ずしも上記実施例に限定されるものではない。

【００３９】

【発明の効果】以上詳細に説明したように、本発明のファイル機密保護装置は、アクセス対象となるファイル自体に当該ファイルへのアクセスを制限するパスワードを格納したため、当該ファイルが格納された記憶媒体の種類に関わらず、アクセスの可否に関する制御を行うことができる。これにより、フロッピーディスクや光磁気ディスクと行った着脱が容易な記憶媒体に格納されたファイルに対しても有効なアクセス制限を行うことができ、機密データを格納することができるという効果がある。

【００４０】また、パスワードをファイル単位で設定できるため、着脱が容易な記憶媒体に格納されたファイルにパスワードを設定した場合であっても、当該記憶媒体中に機密データと非機密データとを混在させることができる。これにより、当該記憶媒体を複数の利用者にて使用する場合に、機密データを扱わない利用者が非機密データに対するアクセスできなくなるという不都合を回避できるという効果がある。

【００４１】さらに、本発明で用いるパスワードは、当該ファイルのデータの一部として当該ファイルに格納されているため、着脱が容易な記憶媒体に格納されたファイルにパスワードを設定して機密データを格納し、本発明のファイル機密保護装置を有しないコンピュータシステムで当該記憶媒体を使用した場合、当該コンピュータシステムではパスワードを設定されたファイルに格納されているデータを正しく読み取ることができず、機密データの機密性が維持される。これにより、確実に機密データの保護ができるという効果がある。

【図面の簡単な説明】

【図１】　本発明の一実施形態によるファイル機密保護装置の構成を示すブロック図である。

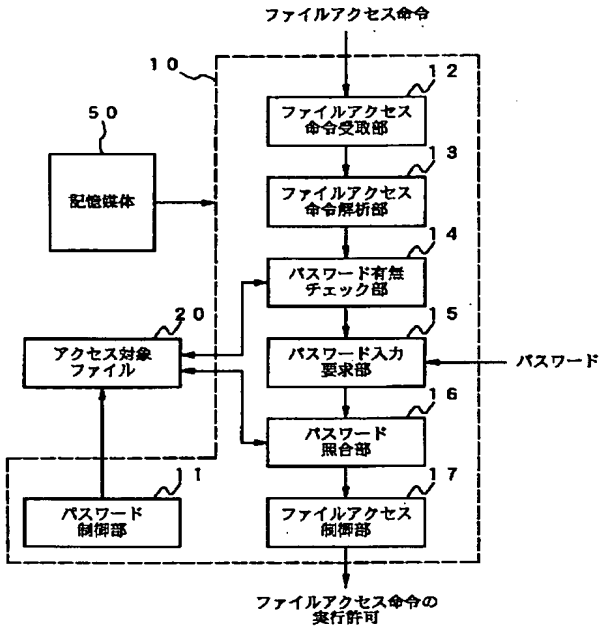
【図２】　本実施形態のファイル機密保護装置を搭載したコンピュータシステムの構成例を示す概略図である。

【図３】　本実施形態のファイル機密保護装置によるアクセス制御動作を示すフローチャートである。

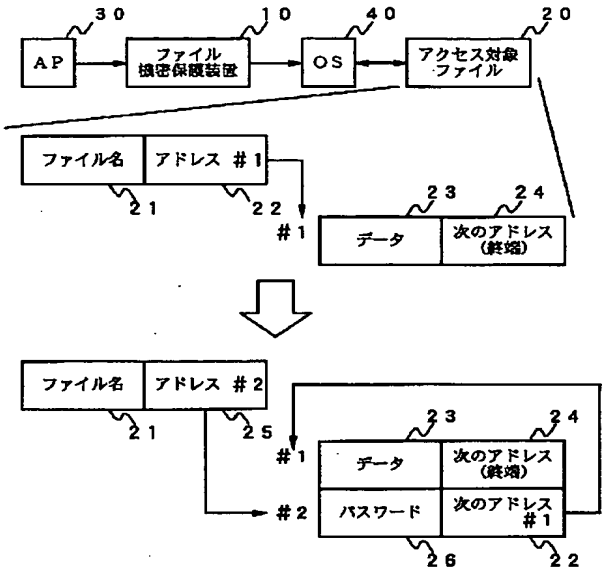
【符号の説明】

１０　ファイル機密保護装置
１１　パスワード制御部
１２　ファイルアクセス命令受取部
１３　ファイルアクセス命令解析部
１４　パスワード有無チェック部
１５　パスワード入力要求部
１６　パスワード照合部
１７　ファイルアクセス制御部
２０　アクセス対象ファイル
３０　アプリケーションプログラム
４０　オペレーティングシステム
５０　記憶媒体

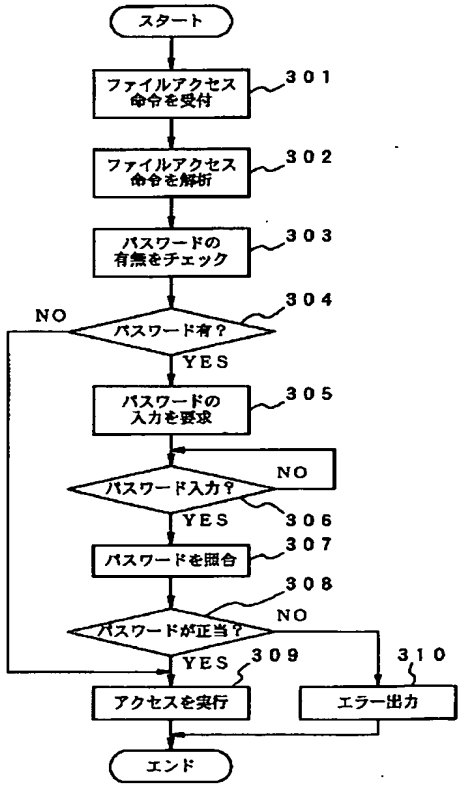
【図１】


ファイルアクセス命令
10
12
ファイルアクセス命令受取部
50
記憶媒体
13
ファイルアクセス命令解析部
14
パスワード有無チェック部
20
アクセス対象ファイル
15
パスワード入力要求部
パスワード
16
パスワード照合部
1
パスワード制御部
17
ファイルアクセス制御部
ファイルアクセス命令の実行許可

【図２】


30
AP
10
ファイル機密保護装置
40
OS
20
アクセス対象ファイル
ファイル名
アドレス #1
21
22
#1
23
24
データ
次のアドレス(終端)
ファイル名
アドレス #2
21
25
#1
#2
データ
次のアドレス(終端)
パスワード
次のアドレス #1
26
22

【図３】


スタート
ファイルアクセス命令を受付
301
ファイルアクセス命令を解析
302
パスワードの有無をチェック
303
304
NO
パスワード有？
YES
パスワードの入力を要求
305
NO
パスワード入力？
306
YES
パスワードを照合
307
308
パスワードが正当？
NO
YES
309
310
アクセスを実行
エラー出力
エンド